AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE RESIDENCE LOCATED AT 26 CHURCH STREET #4, AMELIA, OHIO 45102 [INCLUDING ALL OUTBUILDINGS AND CURTILAGE]

Case No. 1:17MJ -787

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

[SEE ATTACHMENT A]

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

[SEE ATTACHMENT B]

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252 AND 2252A	DISTRIBUTION, TRANSMISSION, RECEIPT, AND/OR POSSESSION OF CHILD PORNOGRAPHY

The application is based on these facts:

[SEE ATTACHED AFFIDAVIT]

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

MARY P. BRAUN, Detective/Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/18/17

Judge's signature

City and state: CINCINNATI, OHIO

HONORABLE KAREN L. LITKOVITZ

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

In the Matter of the Search of:	)	**No.**
	)	
The residence located at	)	
26 Church Street #4	)	**Magistrate Judge**
Amelia, Ohio 45102		
		UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Mary P. Braun, a Detective with the Cincinnati Police Department and a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a Police Specialist with the Cincinnati Police Department since 2004, and for the past seven years have been assigned to the Regional Electronics Computer Investigations (RECI) Task Force working on crimes involving computers and computer based crimes against children and others. I have become familiar with the methods and schemes employed by persons who trade and collect child pornography as well as the manner in which adults seduce children for hands-on offenses. I have investigated federal criminal violations related to crimes against children, child pornography, and human trafficking. I have received formal training in the investigation of these matters at the Cincinnati Police Academy, the Federal Bureau of Investigation, and the National Center for Missing and Exploited Children, through other in-service training, and through private industry. As part of the Federal Bureau of Investigation's Violent Crimes Against Children/Child Exploitation Task Force, in 2011, I was deputized by the United States Marshals Service as a Special Deputy United States Marshal, thereby authorized to seek and execute arrest and search warrants supporting a federal task force.

2. During my career as a Detective and Task Force Officer, I have participated in various investigations involving computer-related offenses and executed numerous search warrants to include those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Task Force Officer, I investigate criminal violations relating to child exploitation and child pornography including the illegal distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

3. As a Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth facts to establish probable cause for a search warrant for the residential property located at 26 Church Street #4, Amelia, Ohio 45102 (the SUBJECT PREMISES). I have not withheld any evidence or information which would negate probable cause.

5. The SUBJECT PREMISES to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A the distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling, all outbuildings and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES

6. Title 18, United States Code § 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct. For purposes of this statute, the term sexually explicit conduct is defined in 18 U.S.C. § 2256(2) as:

A. actual or simulated

i. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
ii. bestiality;
iii. masturbation;
iv. sadistic or masochistic abuse; or
v. lascivious exhibition of the genitals or pubic area of any person."

7. Title 18, United States Code § 2252A makes it a crime to knowingly mail, transport, ship, receive, distribute, reproduce for distribution, sell or possess child pornography in interstate commerce. It also makes it a crime to advertise, distribute or solicit in interstate commerce any material that reflects the belief or is intended to cause another to believe that the material contains an obscene visual depiction of a minor engaging in sexually explicit conduct or a visual depiction of an actual minor engaging in sexually explicit conduct. For purposes of this statute, the term child pornography is defined in 18 U.S.C. § 2256(8) as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

B. such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

C. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. The term sexually explicit conduct has the same meaning as in 18 U.S.C. § 2252, except for the sub-section (B) definition of child pornography where it means:

i. graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

ii. graphic or lascivious simulated; (I) bestiality; (II) masturbation; (III) sadistic or masochistic abuse; or

iii. graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

8. Graphic, when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. *See* 18 U.S.C. § 2256(10).

9. The following terms have the same meanings or explanations in both statutes:

A. "minor" means any person under the age of eighteen years, pursuant to 18 U.S.C. § 2256(1);

B. "visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image, pursuant to 18 U.S.C. § 2256(5);

C. "computer" is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND FILE SHARING PROGRAMS

10. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I have knowledge of the Internet and how it operates. I know that the Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently cross state

and international borders even when the two computers are located in the same state. The following paragraphs describe some of the functions and features of the Internet as it relates to the subject of this search warrant.

11. A website is a collection of Internet pages that Internet users can view. The web address is the name given to a website that enables Internet users to find the website. When a user types in the web address while connected to the Internet, the user will be connected to that website.

12. Many individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP.

13. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log-in files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

14. An Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned a unique IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

15. When a customer logs into the Internet using the service of an ISP, the ISP assigns the computer used by the customer an IP address. The customer's computer retains that IP address for

the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. When an Internet user wishes to visit a website and types the web address into his computer (e.g., www.cnn.com), that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

16. Computers are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including GIF (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

17. Computers are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

18. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer and conducting searches for files

that are currently being shared on another user's computer.

19. The publicly available peer-to-peer file sharing program used in this case allows users to setup their own private P2P network of contacts. File sharing through this particular program is limited only to other users who have been added to your private list of "friends". A new user is added to your list of friends through a "friend request" or "invite". Acceptance of a friend request will allow that new user to download file(s) from the user who sent the friend request. The new user can then browse the list of files the other user has made available to share/download, select the file(s) from this list, and download the selected file(s). The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time.

20. A P2P file transfer is assisted by reference to the IP address. The IP address provides a unique location making it possible for data to be transferred between computers. Once a file has been downloaded, it is stored in the area previously designated by the user for such downloads and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often times a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

21. Third party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

22. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce

23. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer

without his/her permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

24. A computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 100 gigabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

26. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

27. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252 and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

28. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls

within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

c. surveying various files, directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

29. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily- available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and

computer habits.

VII. INVESTIGATION AND PROBABLE CAUSE

30. In February, 2017, your affiant received an investigative lead from Task Force Officer (TFO) Brett Peachey, from the Columbus, Ohio RA of the Federal Bureau of Investigations. TFO Peachey was conducting online internet investigations involving subjects possessing and distributing child pornography using a free publicly available peer-to-peer (P2P) file sharing program. On four separate dates in January, 2017 (1/4/17, 1/5/17, 1/9/17, and 1/10/17) TFO Peachey observed internet protocol (IP) address 174.101.236.244 as a download candidate for suspected child pornography. A query of the files that the computer at the suspect IP address was making available for sharing indicated that the hash values of some of the files matched hash values of suspected or known child pornography files identified by investigators in previous investigations.[1] Hash values of known or suspected child pornography is kept in a law enforcement database. This law enforcement database is compiled from files obtained during previous child pornography investigations. The database allows officers to observe and monitor IP addresses that have been observed to be in possession of or to have distributed digital media files of child pornography via peer to peer networks. The database also provides information regarding when a specific IP address has previously been seen in possession of or disseminating child pornography through peer to peer networks.

31. On the listed dates, the software program utilized by TFO Peachey was able to make a direct connection with a computer utilizing IP address 174.101.236.244 and successfully download 4 images of child pornography. Below is the title and description of the images downloaded by TFO Peachey:

---

1 A hash value is a unique number generated from a larger data source. Hash values have been referred to as electronic "fingerprints" because the numeric values created from a hash function calculation is unique to a very specific piece of data. A change to a single pixel of digital images, for example, would significantly alter the hash value of the image.

CE9551A5379B467EB3BBB2C50628D3C1.jpg: This image shows a prepubescent child lying on her stomach. There is an adult male standing over her with his penis pointed at her. There is a white substance covering the child's buttocks and lower back.

CDBE935E3386A1607778C01E39CC5784.jpg: This image is of a male infant lying on his back. There is an adult male with his hand on the child's penis.

989406636C7D575E7569F300013F52CC.jpg: In this image, a prepubescent female has her mouth on an adult's penis.

F99023252F1BFA11E3DC9C80EF66F2A0.jpg: There are two toddler-aged children in this image. Both of them are leaning their faces against an adult's penis.

32. IP address 174.101.236.244 is resolved to Time Warner Cable. An Administrative Subpoena was served upon Time Warner Cable requesting subscriber information for the above IP address. On or about January 10, 2017, Time Warner Cable responded with information regarding the subscriber of the suspect IP address for the dates and times of the downloaded files described above. The information provided on the suspect IP address is as follows:

Name:	Jerry Wilkinson
Address:	26 Church Street #4, Amelia, Ohio 45102
Email:	onjerry75@twc.com

33. In June, 2017, your affiant received another investigative lead from Detective Don Seamon of the Geauga County, Ohio Sheriff's Office. Detective Seamon was conducting online internet investigations involving subjects possessing and distributing child pornography using a free publicly available peer-to-peer (P2P) file sharing program. On May 15, 2017, Detective Seamon observed internet protocol (IP) address 174.101.236.244 as a download candidate for suspected child pornography.

34. Between May 15 and May 23, 2017, the software program utilized by Detective Seamon was able to make a direct connection with a computer utilizing IP address 174.101.236.244 and successfully downloaded numerous images and videos of child pornography. Below is the title

and description of several of the images downloaded by Detective Seamon:

> **[PTHC]_Dad_fucks_3yo_daughter(1).jpg:** This image shows an infant girl lying on her back. There is an adult's penis pressed against her vaginal area.
>
> **3yo g cum on back.jpg:** There is a toddler-aged child facing away from the camera. There is an adult holding onto his penis and a white substance covering the child's buttocks.
>
> **045.jpg:** In this image there is an adult's penis inside the anus of an infant boy.
>
> **[True pedo zoo] Jenny_01_pthc_Ptsc x_9yo_jenny_enjoying_doggie_cock.jpg:** This is an image of a prepubescent female with her mouth on a canine's penis.

35. Another Administrative Subpoena was served upon Time Warner Cable requesting subscriber information for IP address 174.101.236.244. On or about May 22, 2017, Time Warner Cable responded with information regarding the subscriber of the suspect IP address for the dates and times of the downloaded files described above. The information provided on the suspect IP address is as follows:

Name:	Jerry Wilkinson
Address:	26 Church Street #4, Amelia, Ohio 45102
Email:	onjerry75@twc.com

36. On or about September 12, 2017, your affiant did a RCIC database search on 26 Church Street #4, Amelia, Ohio 45102. The database search revealed that Jerry Wilkinson is listed as a resident of the SUBJECT PREMISES.

37. On or about September 12, 2017, your affiant searched LEADS and learned that Jerry Wilkinson lists the SUBJECT PREMISES as his address on his Ohio Identification Card.

38. On September 29, 2017 at approximately 9:00 AM, your affiant went to the SUBJECT PREMISES and observed the apartment. The building had the number 26 over the front door. Apartment 4 is downstairs on the right hand side of the building.

VIII. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

39. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

A. Those who receive and may be collecting child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

B. Those who receive and may be collecting child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who receive and may be collecting child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist – that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

D. Likewise, those who receive and may be collecting child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

E. Those who receive and may be collecting child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

F. Those who receive and may be collecting child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

G. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

40. Based upon the conduct of individuals involved in the collection of child pornography set forth in the above paragraph, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the SUBJECT PREMISES.

IX. CONCLUSION

41. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that a resident of 26 Church Street #4, Amelia, Ohio 45102 is a collector of child pornography, that violations of Title 18, United States Code, §§ 2252 and 2252A have been committed, and evidence of those violations is located in the premises described in Attachment A. Your affiant respectively requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment B.

REQUEST FOR SEALING

42. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness

Mary P. Braun
Detective/TFO
Cincinnati Police Department/FBI

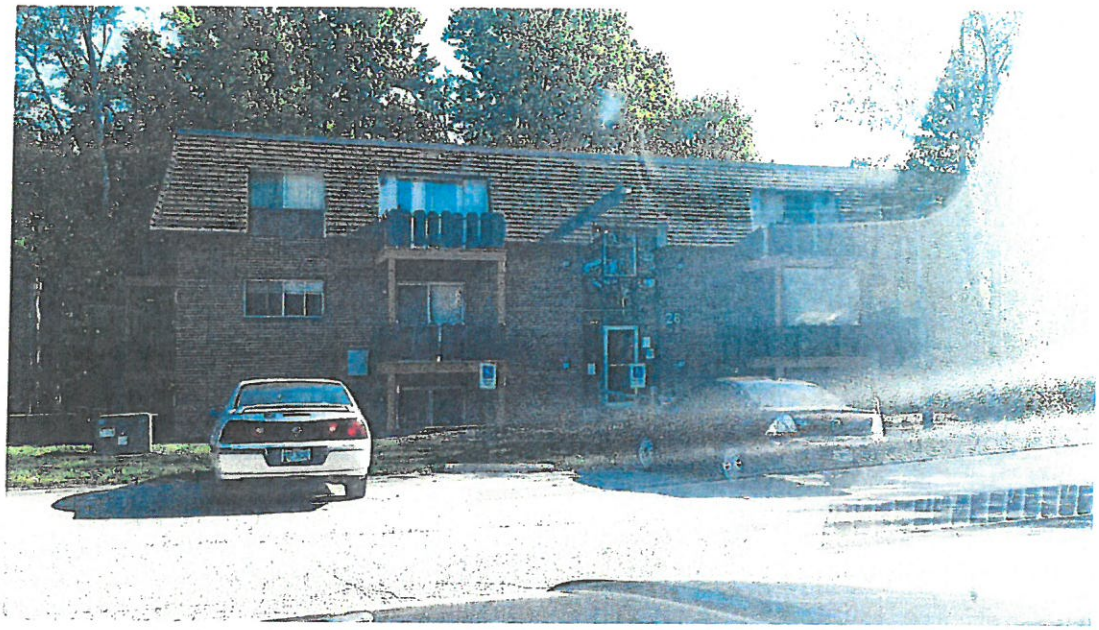
Sworn to and subscribed before me this 18 day of October 2017.

HON. KAREN L. LITKOVITZ
United States Magistrate Judge
Southern District of Ohio

ATTACHMENT A

DESCRIPTION OF PLACE TO BE SEARCHED

The address 26 Church Street #4, Amelia, Ohio 45102 is an apartment on the bottom floor of a 3 story apartment building. The building is brown brick with a glass front door surrounded by several windows. Apartment #4 is down the stairs on the right hand side. The number "4" is clearly marked on the door. There is also a storage area on the same floor, with a locked storage compartment with the number "4" on the front. (See photographs below)



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format or medium, all child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through

interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any evidence of the presence or use of a peer-to-peer file sharing program.